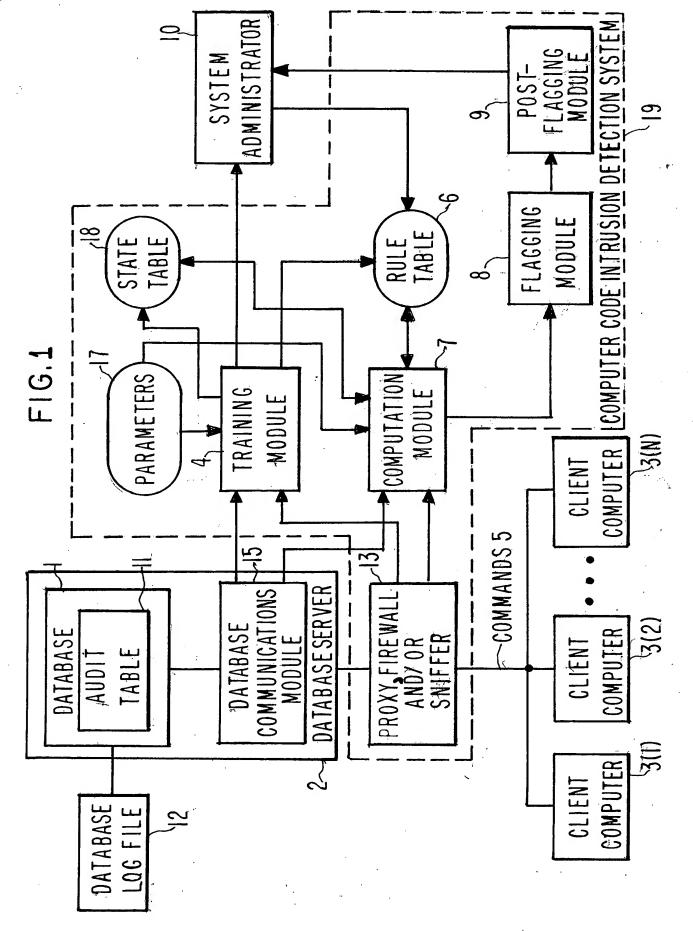
SP 02 MO

U.S. patent application serial #10/632,857 Title: COMPUTER CODE INTRUSION DETECTION SYSTEM BASED ON ACCEPTABLE RETRIEVALS

Inventor: Carey Nachenberg Atty. Docket No.: 20423-07776

Sheet 1 of 5

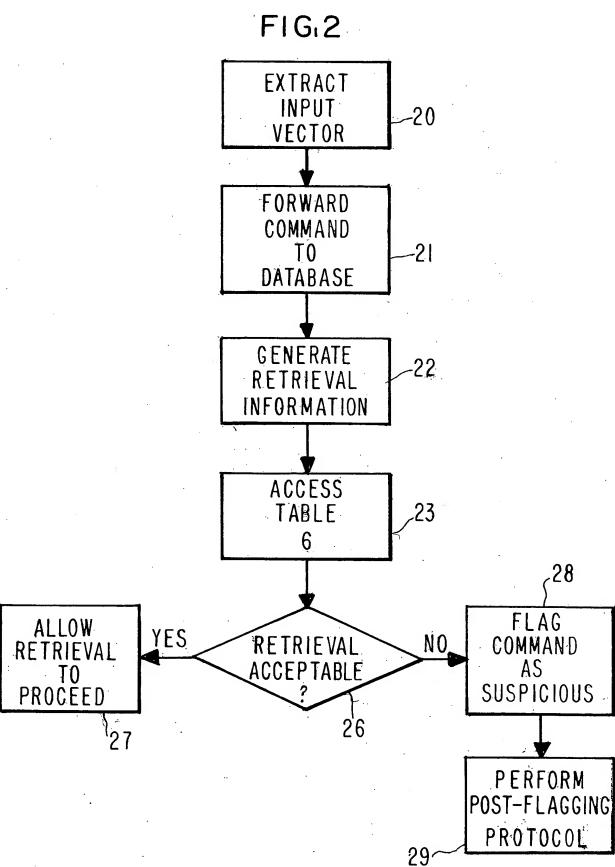


SE O 2 MM DE TO

U.S. patent application serial #10/632,857 Title: COMPUTER CODE INTRUSION DETECTION SYSTEM BASED ON ACCEPTABLE RETRIEVALS

Inventor: Carey Nachenberg Atty. Docket No.: 20423-07776

Sheet 2 of 5



SP 0 2 7003

U.S. patent application serial #10/632,857 Title: COMPUTER CODE INTRUSION DETECTION SYSTEM BASED ON ACCEPTABLE RETRIEVALS

Inventor: Carey Nachenberg Atty. Docket No.: 20423-07776

Sheet 3 of 5

FIG.3

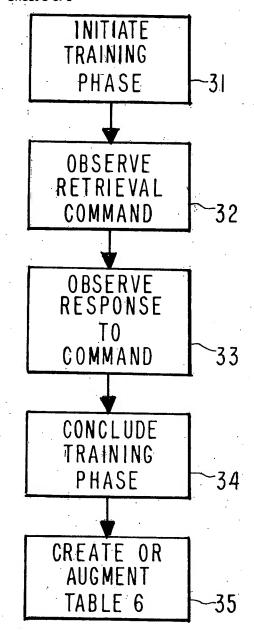


FIG. 4

REPORT
SUSPICIOUS
ACTIVITY
TO SA

TO OPERATIONAL PHASE



U.S. patent application serial #10/632,857
Title: COMPUTER CODE INTRUSION DETECTION
SYSTEM BASED ON ACCEPTABLE RETRIEVALS
Inventor: Carey Nachenberg
Atty. Docket No.: 20423-07776
Sheet 4 of 5

FIG.5

ENTRY #	INPUT VECTOR	RETRIEVAL INFORMATION
1	PRESENT COMMAND	3 COLUMNS COLUMNS A, J, AND K S= 2000 ROWS/SEGOND
2	NONE	D = 2300 COLUMNS/SECOND RATE OF RETRIEVING ROWS WAS
		2000 ROWS/SECOND ACROSS ALL COMMANDS
3	L ₄ F ₁ A ₁	RETRIEVAL VECTOR 1 5 ROWS, 3 COLUMNS - 963 OCCURRENCES
		RETRIEVAL VECTOR 2 7ROWS, 2 COLUMNS - 51 OCCURRENCES S= 1.1 ROW/SECOND D= 23 COLUMNS/SECOND



U.S. patent application serial #10/632,857
Title: COMPUTER CODE INTRUSION DETECTION
SYSTEM BASED ON ACCEPTABLE RETRIEVALS
Inventor: Carey Nachenberg
Atty. Docket No.: 20423-07776
Sheet 5 of 5

FIG.6

ENTRY #	INPUT VECTOR	RULES
1	NONE	RULE 5: NO MORE THAN 1000 ROWS/SEC.CAN EVER BE RETRIEVED BY ANYBODY
2	L ₁ F ₁ A ₁	RULE1: BETWEEN 4 AND 6 ROWS; AND BETWEEN 2 AND 4 COLUMNS ARE ACCEPTABLE RULE 2: BETWEEN 6 AND 8 ROWS; AND BETWEEN I AND 3 COLUMNS ARE ACCEPTABLE RULE 3: S BETWEEN 1.0 AND 1.2 IS ACCEPTABE RULE 4: D BETWEEN 2.2 AND 2.4 IS ACCEPTABLE
3	L ₁	RULE 6: NO RETRIEVALS ARE ALLOWED BETWEEN 6P.M. AND MIDNIGHT UNLESS RULE 7 IS SATISFIED
4	F <u>1</u>	RULE 7: D LESS THAN 10/MINUTE